DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY ALASKA
600 RICHARDSON DRIVE #5000
FORT RICHARDSON, ALASKA 99505-5000

REPLY TO
ATTENTION OF

APVR-RIM 16 July 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: DOIM Policy Statement #8, Special Responsibilities of System and Network Administrators

1. U.S. Army Administrators of information technology bear a heavy responsibility to maximize the availability and utility of the systems they manage while at the same time honoring individual users' justifiable expectations of privacy of information and a communications environment that is "safe" for its users. In addition to having all the responsibilities of any other user as described above, system administrators are granted certain system privileges which make it possible for them to manage the technical resources under their control. System privileges may permit access to initial passwords, files, voice mail, telephone or electronic communication, and information about individual usage patterns. These privileges are necessary for doing their jobs, but have tremendous potential for abuse as well. Such abuse is a violation of 59th Signal Battalion Policy and this section outlines the unique responsibilities and obligations of system and network administrators.

2. These special responsibilities accompany the granting of any network or system privileges to any member of the USARAK community, whether civilian or military. System administrators include individuals who administer DA, USARPAC, USARAK, or 59th Signal Battalion servers; individuals who administer network devices such as modems, switches and routers; individuals responsible for telephone services; and individuals who have any level of privileged access to institutional information systems. Under no circumstances will abuse of system privileges be tolerated. Violations will be considered as legitimate cause for disciplinary action up to and including termination and/or legal prosecution under UCMJ, Joint Ethics Regulations or public law. Individuals not willing to accept these responsibilities should not be in positions which require system privileges in order to perform their duties.

3. In addition, individual systems and servers can be carelessly mismanaged not only to the detriment of the users of that system or service but to the detriment of the entire network. Before making the decision to install a server, the responsible administrator should be prepared to commit the time and resources necessary to ensure proper management. This includes designation of a professional system administrator who will have the time and expertise to understand the technical implications of their systems, stay current on vulnerabilities, software patches and new releases, and be able to address urgent issues on an immediate basis. Failure to do so may endanger not only the integrity of services provided to one's own users but to the USARAK network as a whole. The 59th Signal Battalion will not hesitate to disconnect improperly managed systems that endanger the integrity of institutional networks, systems or

services and it will be the sole responsibility of the unit's system administrator or its command to remedy the situation.

4. While the enclosed list is not considered to be all-inclusive, it establishes the framework for unacceptable behaviors. Commander's have the responsibility to ensure that system administrators within their units address adhere to this policy and should not permit the establishment of servers and services within their units unless they understand the potential for abuse and accept responsibility for compliance. Users should be welcomed to discuss any or all of these matters with their system administrators. All perceived violations of these guidelines should be reported to the 59th Signal Battalion.

FOR THE COMMANDER:

//Original Signed//
GERALD H. MILLER
LTC, SC
Director of Information
Management

DISTRIBUTION:
System Administrators
Network Administrators

USARAK SYSTEM & NETWORK ADMINISTRATOR GUIDELINES

1. System administrators shall protect individual passwords:

Users have the right to expect that their passwords be treated with complete confidentiality. Passwords are never to be divulged to a third party except as necessary in the course of distributing a new password to a user. System administrators should take the utmost care in how passwords are distributed, striving for the best possible balance between a user's needs for privacy and convenience. Anytime a password is transmitted to a user the user should be advised to change their password immediately to protect against any possible disclosure during the transmission.

2. System administrators shall not browse, inspect or copy users' information:

System administrators may not browse the contents of user files or messages -- whether on-line or from backups -- without the user's permission or under direct orders of the DOIM or Commander. Inspection of information is permitted only upon specific authorization from the 59th Signal Battalion or one of its representatives or competent law enforcement personnel such as CID or MPI. As a matter of professionalism, system administrators should avoid direct or indirect contact with users' information and communication content whenever possible. In spite of their best efforts system administrators may from time-to-time encounter confidential information in the performance of their duties. Under no circumstances should such information be acted upon, divulged, or used for the personal benefit or profit of anyone. Violations of this trust endanger the viability of the institutional information infrastructure and will not be permitted. However, system administrators may perform routine scans and are encouraged to utilize standard security tools to check for potentially damaging or illegal software on USARAK networks.

3. System and network administrators shall not routinely collect information on individuals' information usage patterns:

The 59th Signal Battalion expects that the members of its unit will access a rich variety of information and communication resources in the course of their duties. System administrators shall not monitor or collect data regarding the activities of individuals unless specifically authorized to do so in the context of a duly authorized investigation. This is not intended to interfere with the responsibility of system administrators to collect and analyze general anonymous information about the overall patterns of usage of information technology resources. Such information is a vital tool in ensuring the adequacy of the institutional technology environment to meet the needs of its users. System administrators will not disable the routine logging activities that are built into many server operating systems.

4. System administrators shall configure software systems so as to maximize the confidentiality of user communication:

Administrators of email servers in particular bear a responsibility to respect the privacy of their users' communication. Email systems should be configured so as to maximize privacy. For example, email that is rejected for technical reasons should be returned to the sender rather than to the "postmaster." Routine error notification messages to the postmaster should contain only message headers, not the message contents. Users are encouraged to ask their email administrator how email systems are configured and under what circumstance their email may be disclosed.

5. System administrators shall configure systems to enforce appropriate password policies:

All server operating systems will be configured for password security. 59th Signal Battalion system administrators should use these options to comply with the 59th Signal password policy in AR 25-IA (12 Character Minimum, Upper and Lower case, Alpha and Numeric). In addition, system administrators will ensure that all activities relating to security changes are handled in accordance with this written policy and are documented. E.g., system privileges should not be given to individuals who do not need them to perform their job, and the granting of such privileges will be documented. Procedures will be in place for emergency access to critical passwords needed in case of system failure when the usual system administrator(s) is not be available.

6. System administrators shall stay abreast of any vulnerabilities of their systems and manage security in accordance with appropriate recommendations:

System administrators are responsible for remaining up-to-date at all times with security issues relevant to the systems they administer. This may be done through means such as their vendors' information channels or Army Computer Emergency Response Team (ACERT) bulletins. System administrators are required to use this information to apply all recommended security patches in a timely manner as per guidance from the USARAK DOIM, IA Cell.

7. System administrators should configure their systems to minimize the chance for abuse; and act promptly to end abuses upon notification:

Certain kinds of disruptions rely on the naiveté of system administrators on the Internet. Any perception that USARAK is a haven for such abusers endangers the ability of the USARAK network to communicate with others. For example, external sites that have been attacked by someone using a USARAK system as the instrument of the attack may find that they can only safeguard themselves by blocking all traffic from the USARAK network. As just two examples of the kinds of measures that should be taken, email administrators should block anonymous email relays through their systems and network administrators should block the forging of IP source addresses from within networks they manage. As noted above, the DOIM will not hesitate to disconnect improperly managed systems that endanger the integrity of USARAK networks, systems or services and it will be the sole responsibility of the unit's commander and system administrator or its management to remedy the situation.

8. System administrators shall publicize backup policy:

As noted above, backups present a means by which information may be recovered that users believe to have been deleted. Backup policies determine the persistence of deleted information and therefore users have a right to know the backup policy of all systems they use. System administrators should post this policy or make it easily available to their users upon request.

9. No domain administrator has the authority to remove or add personnel to the domain administrator's group without the express approval of USARAK DOIM, 59th Signal Battalion S-3 or the USARAK automation officer.

10. No domain administrator privileges will be granted to anyone who is not assigned to the 59th Signal Battalion.

I have read and I understand fully the duties and requirements of being a network or system administrator on the USARAK Network. Violations of this policy may lead to UCMJ action or dismissal.

*NAME:*__________________________________
(print)

*SIGNATURE:*______________________________ *DATE:*___________________________